Cyber Security – Securing the protection and control relay communication in Substation

Sukumara T
ABB GISLP Ltd.
Bangalore, India
sukumara.t@in.abb.com

Janne Starck
ABB Oy - Finland
Vaasa, Finland
janne.starck@fi.abb.com

Jay Vellore
ABB Inc. - USA
Lake Mary, Florida
jay.vellore@us.abb.com

Eashwar Kumar Harish G
ABB GISLP Ltd.
Bangalore - India
eashwar.r.kumar@in.abb.com
harish.g@in.abb.com

***Abstract*—Protection and control relays (also known as IEDs - Intelligent Electronic Devices), play a critical role in substation protection, control and monitoring functionalities. Smart grid deployments need the seamless flow of data between various devices like protection relays, controllers, gateways, smart meters etc. over private and public communication networks. These kind of deployments lead to inherent requirements for secure communication, strong user authentication and authorization to be considered in the design and development of protection and control relays. Securing relay communication is part of the Defense-In-Depth strategy which is essentially a layered security approach. It uses, multiple layers of network security along with secure architecture which is in-line with current and upcoming cyber security standards to protect the power system/substation automation network against intrusion from physical and cyber-borne attacks while connected to public and private networks. Ensuring confidentiality, integrity and authenticity is an integral part of securing data over the network. This can be achieved with strong authentication and usage of cryptographic protocols like "TLS".**

***Index Terms*— Cyber Security, Substation Automation, Protection and control, Relay/IED Architecture, TLS, Secure Communication.**

I. INTRODUCTION

Protection and control relays, which are the first level intelligent devices in substations, play a critical role in substation protection, control and monitoring functionalities. Relays are an important component of the substation at the bottom of the hierarchical communication network as they have first-hand access to the power systems. They not only play the role of protection which isolates the faulty section of subsystems from the rest of grid but also play an active role in post-fault power restoration and self-healing networks with the help of supported communication network. They aid in the optimized management of substation devices, as well as the overall transmission and distribution power network, which is integral to the smart grid vision and framework. Concepts such as remote configuration/parameterization, remote SCADA communication, remote diagnostics and firmware updates are becoming important requirements for relays. Smart grid deployments need the seamless flow of data between various devices like protection relays, controllers, gateways, smart meters etc. over private and public communication networks. These kind of deployments leads to inherent requirements for Confidentiality, Integrity and Availability (CIA triad part of Information Security concept [1]) of information and data in Substation automation systems network.

The implementation of Ethernet based protocols in the relay and exchange of information over public and private networks have brought huge benefits from an operational perspective, but they have also introduced cyber security concerns previously known only from office or enterprise IT systems. Cyber security risks are inherited as soon as we connect the relay on the Ethernet network.

Securing relay communication is part of the Defense-In-Depth strategy which is essentially a layered security approach. It uses multiple layers of network security to protect the power system/substation automation network against intrusion from physical and cyber-borne attacks while connected to public and private networks. It also highlights importance of development of security architecture and maintaining the architecture design in-line with current and upcoming cyber security standards like NERC CIP regulations, IEEE 1686, IEC 62351 etc. as parts of these standards define the cyber security capabilities to be adapted by relays in the substation and distribution systems. Secure communication, strong user authentication, authorization, logging and reporting have to be considered in the design and development of protection and control relays. This paper covers secure communication design aspects which are a part of overall cyber security architecture in a relay as well as power system network.

II. NETWORK COMMUNICATION AND PROTOCOLS

Communication of relays in Substation and distribution Automation Systems with remote gateways and controllers is mostly through Ethernet and TCP/IP based protocols these days. Some of these protocols are power system domain specific which are used for operation purposes. They facilitate exchange of real-time information continuously and consistently throughout and they are always operational for monitoring and control purposes. Some application protocols are just used for configuration/parameterization, to retrieve data like events/disturbance records for analysis and some basic monitoring for certain period of time.

A. Operation protocols

Protocols such as IEC 61850, Modbus, DNP3, IEC 60870-104 etc. are predominantly used in Substation automation scenario to provide end users with comprehensive real-time information for monitoring and control of power system network. This allows for higher reliability and greater level of control. These systems have become more and more interconnected.

B. Engineering/Configuration and monitoring protocols

The configuration and monitoring tools use application protocols like FTP, HTTP, ODBC etc. to download device configuration, upload firmware, retrieve Disturbance/fault record information etc. Web server support shall use HTTP protocol to connect to remote web client. They also enable connectivity to external networks, such as office intranet and internet.

III. COMMUNICATION SECURITY

With enhanced communication in the transmission and distribution power network, cyber-security becomes an essential part of the overall communication network associated with power system.

The main idea of communication security is to create a secure channel over an unsecure network. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided adequate cipher suites are used and that the server certificate is verified and trusted. A secure product is however not sufficient, as potential vulnerabilities may arise from insecure integration into existing infrastructures. While a substation can form a separate secured island for energy distribution, it must also provide a robust information firewall for parties communicating with the substation and the associated distribution network.

Substation network architecture must be based on the approach of “Defense-in-Depth” which advocates the use of multiple layers of protection to guard against failure of single security component. Secure communication is just one part of this approach (shown in figure 1) [2]. Designing robust security architecture in the relay should also complement with robust and secured network setup when we are connecting our substation system to external internet network.

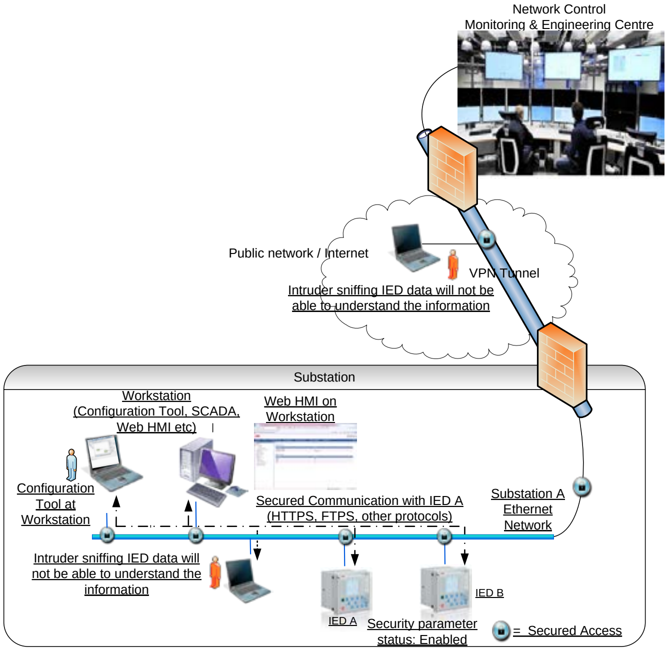
Network Control
Monitoring & Engineering Centre
Public network / Internet
VPN Tunnel
Intruder sniffing IED data will not be able to understand the information
Substation
Workstation (Configuration Tool, SCADA, Web HMI etc)
Web HMI on Workstation
Configuration Tool at Workstation
Secured Communication with IED A (HTTPS, FTPS, other protocols)
Substation A Ethernet Network
Intruder sniffing IED data will not be able to understand the information
IED A
IED B
Security parameter status: Enabled
= Secured Access

Figure 1: Communication through Public Network

A. Standardization in power systems communication security

In Power systems domain, many standardization activities are on-going and cyber security groups are set-up to strengthen security capabilities of critical power infrastructure. Ex: IEC 62351, NERC CIP regulations, IEEE 1686. Some part of these standards define the cyber security capabilities to be adapted by relays in the substation and distribution systems. These standards also enable utilities to effectively and consistently evaluate and benchmark cyber security capabilities of the system/devices.

B. Securing protocols with TLS

The protocols used for engineering the relay and also protocols used for communication between devices have to be secured. Securing data over the network involves ensuring confidentiality, integrity and authenticity. This requires strong authentication and encryption algorithm. There are many security tools available but most famous and widely deployed are “TLS” (Transport Layer Security) and “IPsec” (IP Security).

TLS security protocol based systems are more interoperable compared to IPsec based secured devices [3]. Since Interoperability is an important requirement in Substation and distribution automation domain, TLS based secure communication is a better option for Protection, Control and Monitoring relays. TLS is a protocol that provides a secure channel between two devices. It has facilities for protecting data and identifying the peers. The secure channel is transparent, which means that it passes the data through, unchanged. The data is encrypted between client and server, but the data written at one end is exactly the same as the data read at the other end. Today we have capability to support TLS 1.2 which would be the most secure form as defined in RFC 5246 [7].

TLS is a new network layer that runs in-between applications and TCP/IP. The fact that TLS is a top level network layer has two significant consequences:

- TCP/IP sockets are now used by TLS, on behalf of the higher-level applications
- Application layer modules/protocols like FTP, Web Server, and DNP etc. needs to be specifically designed to use TLS.

The figure 2 shows the secure socket layer introduced between traditional application layer protocols in the power system domain and TCP/IP layer in the network layer architecture.

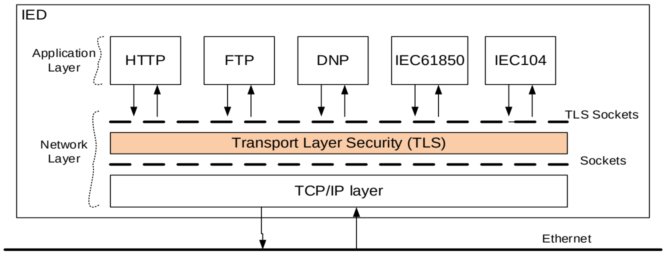

Figure 2: Interface between TLS stack and application protocols

Traditionally Ethernet based application protocols use sockets to access the network layer and in-turn Ethernet network. With secured connectivity option, these socket objects are in-turn taken over by TLS module in order to establish secured channel with proper handshaking process like mutual authentication, key exchange, and further encryption of data packets. This process will be explained further in following chapters.

In the real implementation, there will be a common wrapper for TLS stack with set of common interfaces to provide transparent access to TLS layer. The intermediate TLS wrapper layer provides the abstraction. This wrapper can be extended to support the security of other protocols. This approach enables to adapt the solution in future depending on IEC 62351 standard.

IV. Security Architecture Design in Relay

TLS based secured communication architecture suits relays for Ethernet network based communication design. Apart from secured communication, remote authentication, authorization and security log data transfer also go through the same TLS layer in the relay. Combining strong user access credentials verification along with TLS based communication mechanism provides better security architecture for the relay.

In protection relays, we can add an additional layer for security like option of enabling/disabling secure communication parameter allowed to be set only in local HMI. If this parameter is enabled, then only application protocols like HTTPS and FTPS can be used otherwise both HTTP/HTTPS and FTP/FTPS can be used. This parameter ensures that the local substation has the control and decides on the data exchange mode. If the relay dynamically uses or switches to FTP/HTTP or FTPS/HTTPS depending on the request from the remote client (without the parameter), then the remote client could control on the decision of secured and non-secured mode option which is dangerous. Also this parameter enables substation operational maintenance engineers to disable security while carrying out commissioning and maintenance work.

“Input validation” at the first/entry point of application layer is another critical point to be adopted in the secure relay design.

These steps are to be part of Defense-In-Depth approach with-in the design and implementation of Cyber-security architecture for relays.

Cyber security feature takes considerable system resources like CPU power, memory, bandwidth etc. The relay architecture needs to consider these characteristics and constraints and optimize the design such that the system performance, availability and reliability are maintained while supporting the cyber security features.

A. TLS handshake

From the perspective of information exchange over Ethernet network, relays in the substation are one of the primary sources of information. Relays provide real time data to local and remote clients like SCADA systems, Control Centers, web clients etc. So naturally from network socket communication perspective, relays acts as socket servers and remote systems are socket clients.

Normally application protocol modules are started during relay initialization/start-up which create and bind local address to the sockets and waiting for valid remote client connection requests on specific ports on the Ethernet network. Once valid the connection request comes from remote clients, the server starts accepting the request, creates the socket objects and passes these objects to the TLS communication interfaces. Now TLS stack starts the hand shaking process. The figure 3 sequence diagram shows how application modules like HTTPS and FTPS initiate secure connection in order to exchange the information. The exchange of information like TLS version support, cipher suit selection, key exchange and certification handling are part of this handshaking process. Once successful handshaking is done, a valid and secure session is created for further data exchange. The TLS handshaking process is an independent activity and each application module/session will have a separate handshaking process with in the relay.

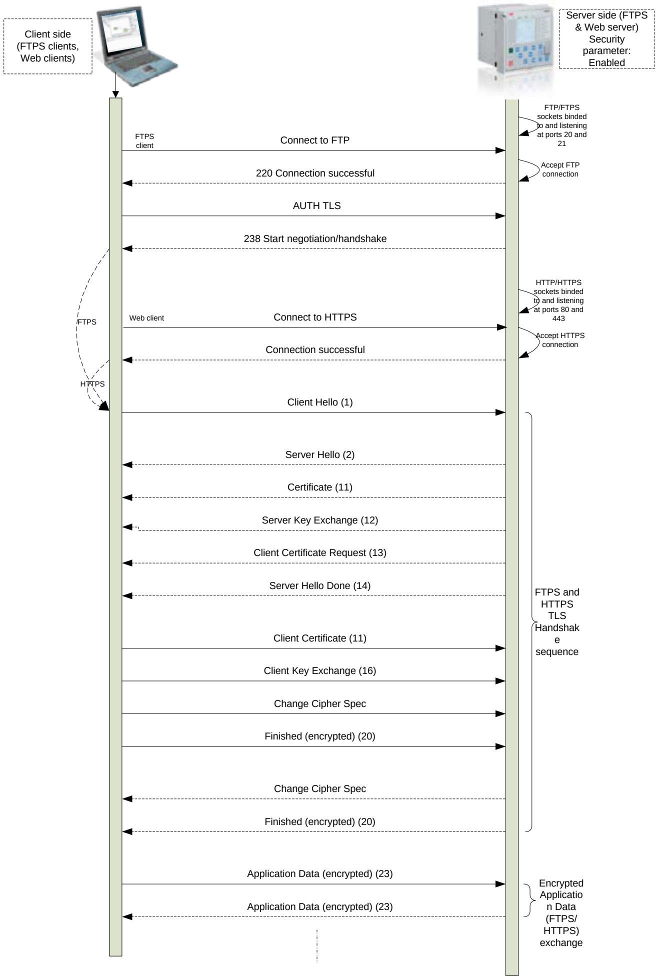
Client side (FTPS clients, Web clients)
Server side (FTPS & Web server) Security parameter: Enabled
FTP/FTPS sockets binded to and listening at ports 20 and 21
FTPS client
Connect to FTP
Accept FTP connection
220 Connection successful
AUTH TLS
238 Start negotiation/handshake
HTTP/HTTPS sockets binded to and listening at ports 80 and 443
FTPS
Web client
Connect to HTTPS
Accept HTTPS connection
Connection successful
HTTPS
Client Hello (1)
Server Hello (2)
Certificate (11)
Server Key Exchange (12)
Client Certificate Request (13)
Server Hello Done (14)
FTPS and HTTPS TLS Handshake sequence
Client Certificate (11)
Client Key Exchange (16)
Change Cipher Spec
Finished (encrypted) (20)
Change Cipher Spec
Finished (encrypted) (20)
Application Data (encrypted) (23)
Application Data (encrypted) (23)
Encrypted Application Data (FTPS/ HTTPS) exchange

Figure 3: TLS Handshaking Process

The TLS handshaking and session set-up is a CPU intensive operation. For SCADA protocol modules like DNP, Modbus TCP and IEC61850, handshaking process shall only be in the beginning of the connection as the session is expected to be continuous. On the other hand configuration/engineering protocol modules like FTPS and HTTPS, the handshaking process could be more often as the data transfer is not continuous and only based on user request/operation.

B. Certificate handling

Certificates in secured communication shall be used to validate / authenticate the client and server before exchanging the information. Certificates use the asymmetric cryptography (Uses two different types of cryptographic keys public key and private key) so that we can encrypt the information with one key and decrypt it with the complement key from a given public-private key pair. Certificate provides the identity of the owner and public key for communication. Certificates will be issued by the trusted Certificate Authority (CA) for limited time. Certificates can be created with the third party certificate authority or themselves as certificate authority known as self-generating/self-signed certificates.

During TLS handshaking process (as shown in fig 3), server issues the certificate to the client after “server hello” message and request for the client certificate. If some application functions mandate client certificate validation, server can also request for the client certificate. If client certificate is not received, server can close the connection. Client validates the server certificate with the known list of the certificate authority. If the certificate authority of the server certificate is not listed then client will display a warning. It is up to the user to go ahead with the connection or install the certificate as the trusted root certificates.

In a substation automation/power system network, before a system makes a secure connection to a relay over a network, a valid TLS certificate must be installed / available in the relay. A TLS certificate can be either self-signed certificate or a trusted CA certificate. A self-signed certificate is an authentication mechanism that is created and authenticated by the system on which it resides. The relay could generate its own self signed certificate or the trusted static CA certificate could be ported / stored in the relay’s flash memory.

C. Secured relay configuraton and monitoring with TLS

Relay configuration and monitoring tools normally use FTP protocol for transferring device configuration information, transferring disturbance record data, trend/load profile data, history log and operation events information. Relays also support basic parameterization, control and monitoring through web-clients using HTTP protocol. Also concepts like remote diagnostics, configuration and maintenance services are catching-up in power systems automation domain. Hence it is essential to secure the protocols used for above purposes.

Let us now take a typical FTP and HTTP application protocols implementation in a relay and how these protocols are secured with TLS. Secured version of these protocols are called FTPS and HTTPS respectively.

FTPS (also known as FTP Secure and FTP-TLS) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS 1.x) cryptographic protocols.

There are two different modes in FTPS to transfer the files secured over the network, they are:

- FTPS (explicit) - In explicit mode (also known as FTPES), an FTPS client must "explicitly request" security from an FTPS server and then step-up to a mutually agreed encryption method. If a client does not request security, the FTPS server can either allow the client to continue insecure or refuse/limit the connection.
- FTPS (Implicit) –In Implicit mode, A client is immediately expected to challenge the FTPS server with a TLS Client Hello message. If such a

message is not received by the FTPS server, the server should drop the connection.

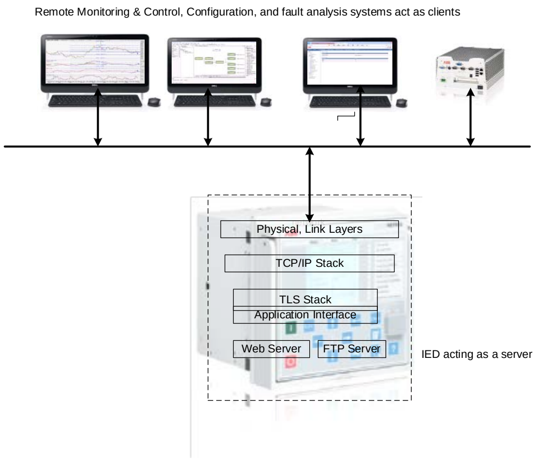

Figure 4: FTPS and HTTPS implementation overview

Hypertext Transfer Protocol Secure (HTTPS) is a combination of Hypertext Transfer Protocol (HTTP) with TLS protocol. It provides encrypted communication and secure identification of IED's web server.

Implementation for these protocols in the relay as shown in figure 5 should be such that both secured and non-secured versions should be supported and customer or utility should be able to configure/select either of these versions based on the project requirements. If secure communication option is disabled but the clients wants to connect via secured mode, implementation should support the same. But vice versa should not be supported.

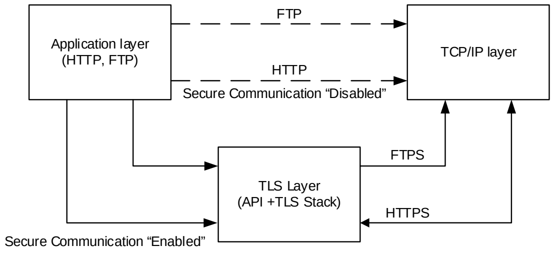

Figure 4 Re-routing of calls

D. FTPS implementation

FTPS Implementation includes adding of additional commands & responses over the normal FTP (Implementation done as per [5] & [6]). Certain modification have been done to suit to the substation environment which are explained further. Explicit mode of FTPS is implemented and covered here. FTPS server in relay will not support simultaneously both "Normal Mode" and "Secured mode" (Explicit mode connection). An extra configuration parameter is added to select the transfer type (as either Secured mode or unsecured mode).

User / Administrator should enable the type of communication (Secured / Unsecured). If user feels that communication inside the substation should be secured (Configure the communication as secured) then it is mandatory for the client to establish the secure communication (Implicit / Explicit FTPS connection). If the client requests for the normal FTP connection, then the connection will be rejected. If the user configures the communication as unsecured then both normal FTP/FTPS connection will be allowed.

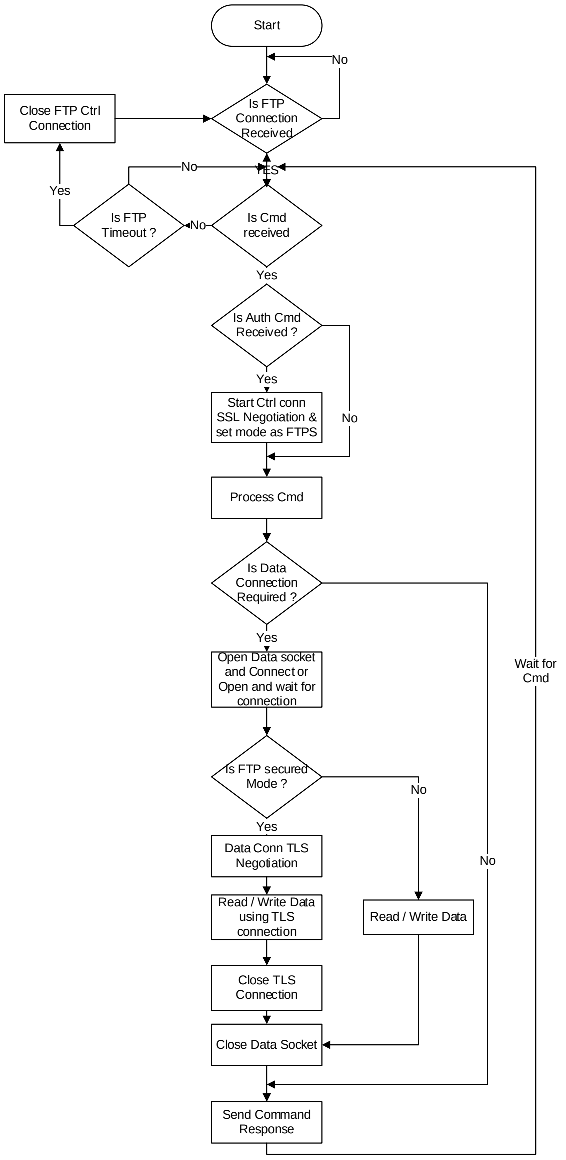
Start
No
Is FTP Connection Received
Close FTP Ctrl Connection
No
YES
Yes
Is FTP Timeout ?
No
Is Cmd received
Yes
Is Auth Cmd Received ?
Yes
Start Ctrl conn SSL Negotiation & set mode as FTPS
No
Process Cmd
Is Data Connection Required ?
Yes
Open Data socket and Connect or Open and wait for connection
Is FTP secured Mode ?
No
Yes
Data Conn TLS Negotiation
Read / Write Data using TLS connection
Read / Write Data
Close TLS Connection
Close Data Socket
Send Command Response
No
Wait for Cmd

Figure 6 FTPS Functional Overview flow chart

The figure 6 provides the overview of the FTPS server (Explicit Mode) implementation in relays.

The server will open FTP control socket on port 21 and will be waiting for connection from client. Once the connection is established from client. Client will send the commands to perform file transfer functions.

The FTPS server can support both Normal FTP mode as well as Explicit FTPS mode. In the case of Normal FTP mode, data will be transferred as clear text on both control channel and data channel. In Explicit FTPS mode, data will be encrypted and sent over data and control channel.

Client sends AUTH command in Explicit FTPS mode to perform TLS negotiation on control channel and make control channel secured. Once the negotiation is completed, FTPS server sets the state as Explicit FTPS mode. Then further FTPS/application level user name and password is validated. If client request for file transfer in explicit FTPS mode, the data connection shall be established as per the FTP mode set (ACTIVE / PASSIVE) and TLS negotiation will be performed on data channel to have secured data channel. Data will be transferred on this channel. Data channel and socket will be closed once the data transfer is complete.

Control channel will be active until FTP session is closed or FTP timeout is expired.

E. HTTPS implementation

The HTTPS implementation mainly involves updating HTTP web server stack of the relay to be able to handle HTTPS by introducing a TLS layer between the HTTP and TCP/IP layers [4].

HTTP/HTTPS operation is activated based on the Security parameter which is used primarily to enable the sub-station (via the LHMI) to maintain control over what type of connection will be allowed between the web server and the web client.

If the Security parameter is disabled, then the web server will respond to both HTTP and HTTPS requests on port 80. If the Security parameter is enabled, then the web server will respond only to HTTPS requests on port 443. But there is no way for a user logging in from a web browser to know before logging into the Web HMI as to whether the Security parameter is disabled or enabled. In other words the web client (web browser) will not know whether to connect to port 80 or port 443. The solution to this problem is configuring the web server to listen to both ports 80 and 443. Whenever the web client request comes to port 80 when security is enabled, the server will redirect this request to the port 443.

So when the user opens a browser window and just types the IP address (without specifying the port number or the protocol – HTTP or HTTPS), the browser will assume HTTP by default and will send a request to port 80 of the web server. If the Security parameter is disabled, then the web server will log the user into the web server over HTTP after application level authentication like checking the user access credentials and rights. Otherwise, if the Security parameter is enabled, then the web server will redirect the request to port 443 where the web server will first perform the TLS handshake, and then log the user into the web server over HTTPS after authentication validation process as mentioned above. At the same time the relay will respond to requests on port 443 also in addition to port 80 when the Security parameter is disabled. User should always have the choice to use secure communication irrespective of the parameter.

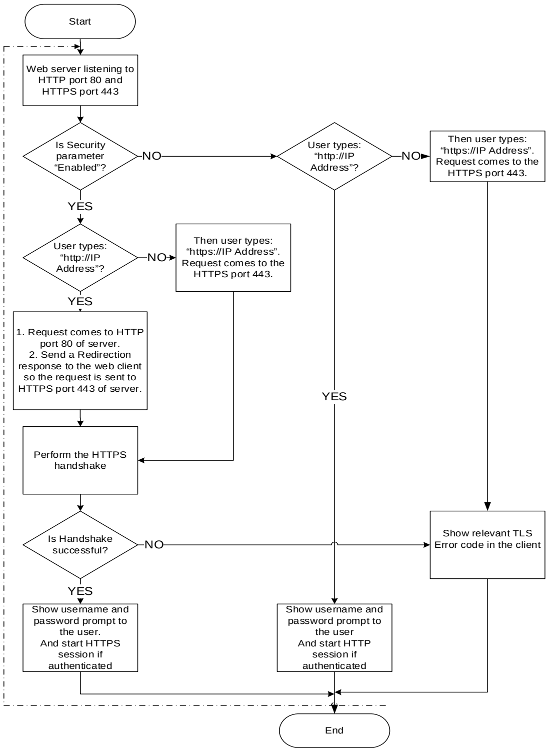
Start
Web server listening to HTTP port 80 and HTTPS port 443
Is Security parameter "Enabled"?
NO
YES
User types: "http://IP Address"?
NO
Then user types: "https://IP Address". Request comes to the HTTPS port 443.
YES
1. Request comes to HTTP port 80 of server.
2. Send a Redirection response to the web client so the request is sent to HTTPS port 443 of server.
Perform the HTTPS handshake
Is Handshake successful?
NO
YES
Show username and password prompt to the user.
And start HTTPS session if authenticated
User types: "http://IP Address"?
NO
Then user types: "https://IP Address". Request comes to the HTTPS port 443.
YES
Show relevant TLS Error code in the client
Show username and password prompt to the user
And start HTTP session if authenticated
End

Figure 5 HTTPS Functional Overview flow chart

There is a common authentication mechanism within the relay which is applicable for both HTTP and HTTPS. Web server module and related application modules in the relay provide functionality like support for monitoring information, parameter configuration and disturbance record downloads. The HTTPS implementation takes full advantage of the layered architecture of the relay with almost no impact on the other layers especially application layer protocols and functionalities.

F. Managing system resources

In a secure communication process, each remote client session (like FTPS, HTTPS sessions) makes an independent connection with corresponding server module in the relay. Normally the runtime memory consumption is high during "TLS handshaking" process. Once the secure connection is established the memory consumption will be considerably less than the peak runtime memory consumed during handshake process. The relay architecture designs need to consider how many secure application protocol sessions can be supported with available system resources like runtime memory and CPU processing capability, bandwidth etc.

V. Conclusion

The secured communication mechanism can be developed using available security technologies and seamlessly integrate it to relay architecture to realize certain cyber security requirements. It's true that Cyber security environment is most dynamic and development efforts should be constantly vigilant and check for technology trend and re-build strong security mechanisms and "defense-in-depth" strategy will need to be applied where each system component is an active participant in the creation of secured system in order to overcome the threats to make strong and robust power system networks.

References

[1] Jacques Benoit, Meeting IED Integration Cyber Security Challenges: Eskom Southern Africa Power System Protection Conference; November 12-14, 2008

[2] Markus Braendle, Steven A. Kunsman, White paper Balancing the Demands of Reliability and Security Cyber Security for substation Automation, Protection and Control Systems

[3] AbdelNasir Alshamsi, Takamichi Saito ,A Technical Comparison of IPSec and SSL: Tokyo University of Technology:19th International Conference on Advanced Information Networking and Applications;2005.

[4] [RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000, http://www.ietf.org/rfc/rfc2818.txt

[5] [RFC4217] Ford-Hutchinson, P., "Securing FTP with TLS", RFC 4217, October 2005, http://www.ietf.org/rfc/rfc4217.txt

[6] [RFC2228] Horowitz, M., and Lunt, S., "FTP Security Extensions", RFC 2228, October 1997, http://www.ietf.org/rfc/rfc2228.txt

[7] [RFC 5246]